AMANO Time Stamp Service Type-Free-A

運用規程（TP/TPS）

Version 1.3

2010 年 10 月 1 日

アマノビジネスソリューションズ株式会社

目次

改版履歴

初版発行日：2006 年 8 月 23 日

版	変更日	内容
Ver 1.1	2009/01/20	1. 「8.タイムスタンプトークンのプロファイル」における TSTInfo の ordaring の設定値を変更
Ver 1.2	2010/05/10	1. 「1.2.2　オブジェクト識別子」において、本サービスにおいて使用される時刻源を変更 2. 「1.3.2　関係者」において、利用する時刻配信局を変更 3. 「1.4　所在地」住所変更
Ver 1.3	2010/10/01	1. 会社・組織名称をアマノタイムビジネス株式会社からアマノビジネスソリューションズ株式会社に変更 2. 「1.4　本規程に関する連絡先の詳細」の E-MAIL フォームの URL を変更

1. はじめに

AMANO Time Stamp Service Type-Free-A は、タイムスタンプ局（以下「TSA」と言う）として電子データに信頼のおける時刻のタイムスタンプを付与するサービス(以下「本サービス」と言う）であり、AMANO Time Stamp Service Type-Free-A 運用規程（以下「本規程」と言う）では、アマノビジネスソリューションズ株式会社 (以下「アマノビジネスソリューションズ」と言う）が本サービスを利用者に提供する為の運営方針を述べる。

尚、本規程の構成は、IETF PKIX による RFC2527「Certificate Policy and Certification Practices Statement Framework」を参考としている。

1.1 概要

タイムスタンプは、ある電子データの「存在証明」や「非改ざん証明」を行う場合に非常に有効な手法である。本サービスは、信頼のおけるタイムソースと公開鍵暗号技術を用いた高度な仕組みを採用し、利用者にとって簡単、安価、迅速に利用出来るものとして提供する。

しかしながらこの有効性を確保するには以下の条件が必要である。

（１）利用するタイムソースが信頼のおけるものである事。
　　ここで信頼がおけるとは国家時刻標準機関との追跡性が確保されている事を言う。

（２）タイムソース及びデジタルタイムスタンプの生成、検証に関わる設備の信頼性や安全対策の確保。

（３）秘密鍵、検証鍵の管理に代表される運用管理体制の信頼性の確保。

（４）タイムスタンプ方式自体が持つ信頼性と強度の確保。

（５）運営主体及び利用者の義務と責任の遂行。

本規程は、上記一連の信頼の鎖を途切れる事無く確保する為に、重要な要件に関して可能な限り明確化し、実行する事を文書化するとともに公開する本サービスを運用する TSA（以下「本 TSA」と言う）の宣言書である。

なお、本 TSA は、タイムスタンプポリシー（Time-stamp policy）及び TSA 運用規程（Time-stamping practice statement）をそれぞれ独立したものとせず、本規程を本 TSA の本サービスに関する運用方針として位置づける。

1.1.1 本規程の位置づけ（定義）

本規程は、本 TSA 及びそれが提供する本サービス「AMANO Time Stamp Service Type-Free-A」の運用方針について定めたものである。また、本 TSA 並びに本サービスの業務に携わる社員及び協働者はこれに従い業務を遂行しなければならない。

1.2 識別

1.2.1 ドキュメント名称、バージョン

ドキュメント名称：AMANO Time Stamp Service Type-Free-A 運用規程

バージョン：1.3
作成日：2010 年 10 月 1 日
作成者：アマノビジネスソリューションズ株式会社

1.2.2 オブジェクト識別子

内容		OID
本サービス		
	アマノビジネスソリューションズ株式会社	0.2.440.200217
	AMANO Time Stamp Service Type-Free-A	0.2.440.200217.100.200
	サービスポリシー	0.2.440.200217.100.200.100
本サービスにおいて使用される認証局		
	AMANO RootCA for TA/TSA	0.2.440.200217.100.10
本サービスにおいて使用される時刻源		
	アマノ時刻配信･監査サービス for TSU	0.2.440.200192.100.100
	サービスポリシー	0.2.440.200192.100.100.100

1.3 コミュニティーと適用性

1.3.1 適用範囲と対象

本規程の適用範囲は、本 TSA 及び本サービスの運用、その情報を扱う業務全般である。また、本規程の適用対象は本 TSA 並びに本サービスの全ての利用者、及び本サービスに関係する法人、個人、組織を含む。

1.3.2 関係者

（1）タイムスタンプ局（TSA）

本規程において TSA とは、RFC3161 に基づくタイムスタンプトークン発行業務を行う事業者、すなわち本 TSA の事を言う。

（2）社員

本規程において社員とは、アマノビジネスソリューションズの社員及び嘱託者の事を言う。

（3）申請者

本規程において申請者とは、TSA の提供するサービスへの加入申請を行った者の事を言う。

（4）利用者

本規程において利用者とは、TSA の提供するサービスへの加入申請を行い TSA からサービスへの加入を認められ、そのサービスを受ける対象装置を所有、管理、又は使用する者の事を言う。あるいは、加入申請が必要で無いサービスの場合は、AMANO

Time Stamp Service Type-Free-A 利用規約（以下「利用規約」と言う）に同意して利用する者の事を言う。

（５）協働者

本規程において協働者とは、アマノビジネスソリューションズと雇用関係を持たず、契約等によって定められた範囲において TSA の業務を支援する者の事を言う。

（６）第三者

本規程において第三者とは、TSA、社員、協働者以外の個人、法人の事を言う。

（７）時刻配信局（TA）

本規程において時刻配信局とは、UTC に対してトレーサビリティのある時刻の配信を行い、かつ TSA が管理するタイムスタンプユニット内の時計の時刻監査を行う事業者をいう。本 TSA はアマノ株式会社が運営するアマノ時刻配信・監査サービス for TSU（以下「当該 TA」と言う）を利用する。

（８）認証局（CA）

本規程において認証局とは、TSA のタイムスタンプユニットに使われる公開鍵証明書の認証を行う事業者をいう。本 TSA の認証局は AMANO RootCA for TA/TSA とする。

1.3.3　本サービスの概要

本 TSA は、利用者からのタイムスタンプトークン発行要求に対して RFC3161 に準拠したタイムスタンプトークンを生成し、発行する。

（１）本 TSA は、タイムスタンプの対象となるデータの内容については一切関知しない。

（２）タイムスタンプトークンに含まれる時刻情報は、TSA がタイムスタンプトークンを生成した時点の時刻とする。

（３）タイムスタンプトークンの有効期間は、10 年間とする。但し、秘密鍵の危殆化やハッシュ及び暗号アルゴリズムの脆弱化が発生した場合には、タイムスタンプトークン示される有効期限より以前に、その有効性を失効させる事がある。

（４）タイムスタンプトークンの生成に使用されるハッシュアルゴリズムは、SHA-1/SHA-256/SHA-384/SHA-512 とし、タイムスタンプ対象データに対するハッシュ値を計算したアルゴリズムと同じものが適用される。

1.4　本規程に関する連絡先の詳細

組織名称　　：アマノビジネスソリューションズ株式会社

所在地　　：〒222-0011 神奈川県横浜市港北区菊名 7 丁目 3 番 24 号

E-MAIL フォーム ：　http://www.e-timing.ne.jp/tsa/purchase/inquiry.html

2. 一般規定

2.1 義務

2.1.1 TSA の義務

（1）本 TSA は、本 TSA 及び本サービスの信頼性と安全性の確保を行う。

（2）本 TSA は、本規程に従い、タイムスタンプサービスとして、タイムスタンプトークンの発行サービスを提供する。

（3）本 TSA は、本規程に従い、本 TSA で使用する秘密鍵、公開鍵を安全に生成し管理する。

（4）本 TSA は、秘密鍵、公開鍵を定期的に更新する。万一危殆化が判明した場合は、その鍵を使ったタイムスタンプトークンの発行を中止し、認証局への連絡及び公開鍵証明書の失効手続きを行うとともにサービス利用者へ通知を行う。

（5）本 TSA は、サービス利用者の義務について周知させるとともにその履行に必要な各種情報を必要に応じて提供する。

2.1.2 サービス利用者の義務

（1）利用者は、本規程及び利用規約に了承した上で本サービスの提供を受けるものとする。

（2）利用者は、サービス利用の申請などに際し、正確な情報を本 TSA に提示するものとする。

（3）利用者は、本サービスの利用に際し利用者側で使用するソフトウェア、機器類に対しては自己の責任と判断の下に利用し安全対策などの一切の必要な管理を行う。

2.2 責任

2.2.1 TSA の責任

本 TSA は、運営を維持しかつその義務を履行する為に必要な財政的基盤を有するものとする。

2.2.2 利用者の責任

利用者は、タイムスタンプを検証した第三者に対し、本規程の「2.1.2　サービス利用者の義務」で定められた内容に反して本サービスを利用した事から発生する全ての責任を負う。但し、これは、本規程で定める利用者の他の責任及び義務を制限するものでは無い。

2.2.3 財務的な責任

アマノビジネスソリューションズは、本規程の「2.2.1　TSA の責任」に違反して損害賠償責任を負う場合、利用規約に従うものとし、いかなる場合においてもアマノビジネスソリューションズはこの賠償額の上限を超える責任を負うものでは無い。利用者が本規程に定める義務を履行せず、又は本規程の「2.2.2　利用者の責任」で定める責任に違反した事によりア

マノビジネスソリューションズが損害を被った場合、アマノビジネスソリューションズは利用者に対し当該損害の賠償を請求する事が出来る。

2.3　免責事項

アマノビジネスソリューションズは、利用者が本サービスを使用するにあたっての利用者自身のシステムに起因するあらゆる損失、損害又は費用については免責される。アマノビジネスソリューションズは、アマノビジネスソリューションズの責任に帰する事が出来ない事由から生じた損害、及び予見の有無を問わず特別の事情から生じた損害については免責される。その他の免責事項及び賠償責任の限定については利用規約に従うものとする。

2.4　解釈と執行

2.4.1　準拠法

当事者間の契約又は他の法規選択にかかわりなく、本規程の適用、構成、解釈、妥当性等は、日本法に準拠する。

2.4.2　可分性

本規程のある規定もしくはその一部、あるいはその適用が、何らかの理由により無効又は執行不可能であると判明した場合は、その規程又はその範囲のみが無効又は執行不可能となり、その他の部分は有効でありかつ適用される。

2.4.3　存続性

本規程の「2.2.3　財務的な責任」、「2.3　免責事項」、「2.4　解釈と執行」、「2.7　守秘性のポリシー」、「2.8　知的財産権」及び「2.9　個人情報の扱い」は、本TSAによる本サービスが終了し、本規程の廃止後も有効に存続する。

2.4.4　承継

本規程は、明示、黙示、表見上に関わらず、双方当事者の承継者、遺言執行者、相続人、代表者、管理者及び譲受人の利益となり、また拘束する。

2.4.5　通知

本規程に関する通知は書面、又は電子メールにて本規程の「1.4　本規程に関する連絡先の詳細」にある連絡先で受け付ける。通常は受領日をもってその通知は有効となるが、当該通知に受領日以降の日付がある場合にはこの限りでは無い。本 TSA から利用者に対し通知が必要と判断される場合には、登録されている連絡先へ通知を行う。

2.4.6　紛争解決の手続き

本規程又はそれに付随して生じた紛争、本TSAによる本サービスに関する紛争について法廷での解決を図る際、東京地方裁判所が第一審の専属的合意管轄裁判所となる。

2.4.7　不可抗力

アマノビジネスソリューションズは、天災、戦争、伝染病、停電、火災、地震、テロ、その他の災害など、アマノビジネスソリューションズの支配を超える事件から生じた本規程に関する違反、遅滞、不履行に、一切責任を負わない。

2.4.8　解釈

特に他の規定が無ければ、本規程はあらゆる状況の下で商業的な妥当性と合理性を失う事の無いように解釈すべきものとする。本規程を解釈するにあたっては、国際的な視野や目的、その目的で一貫性を押し進める利益、誠実な履行を考慮する。

2.4.9　権利放棄の禁止

本規程の違反に関してのアマノビジネスソリューションズ又は利用者の権利放棄は、書面によって行うが、いかなる場合もその後に生じる規程違反に関しての権利放棄やその規定そのものの権利放棄と解釈してはならない。

2.5　料金

規定しない。

2.6 公表とリポジトリ

2.6.1　TSA に関する情報の公開

本 TSA は、本規程をリポジトリに公開する。

2.6.2　公開の時期

本 TSA は、本規程変更時、その他本 TSA の責任者が必要と判断した際に随時更新を行う。

2.6.3　アクセス制御

本 TSA のリポジトリには、インターネットでアクセス出来る。特にアクセスの制御は行わない。

2.6.4　TSA のリポジトリ

本規程は、下記の URL における本 TSA のリポジトリで参照出来る。

URL：https://www.e-timing.ne.jp/repository/tsa/tfa_repository.html

2.7　守秘性のポリシー

2.7.1　機密扱いとみなす情報

本 TSA 及び利用者は、その情報が漏えいする事によって本 TSA 及び利用者の信頼性、適格性が損なわれる恐れのある情報を機密扱いとする。本 TSA により機密扱いとみなされた情報は、本 TSA により安全に保管、管理され、本規程又は利用規約に定められている場合を除いては、いかなる者にも原則開示しない。

2.7.2　機密扱いとみなさない情報

「2.7.1　機密扱いとみなす情報」の規定に関わらず、本TSAは次に定める情報については機密扱いとはみなさない。

（１）本規程等公開情報として明示するもの。
（２）利用者又は本TSAに開示後、本TSAの責任の範囲外で公知となった情報。
（３）合法的に入手し、かつ利用者又は第三者から機密保持の義務を負っていない情報。
（４）利用者又は本TSAが第三者に対し機密保持の義務を課す事無く開示した情報。
（５）個人的に識別可能な全ての情報を除き、その情報の元の所有者を識別出来なくした統計目的で編集したデータ。

2.7.3　法執行機関への情報開示

本TSAは、本TSAで扱う全ての情報に対し法的根拠に基づく情報開示の要求が法執行機関よりなされた場合、法で定められた範囲内で当該情報の開示を行う。

2.7.4　民事手続き上の情報開示

本TSAは、本TSAで扱う全ての情報に対し、訴訟、調停、その他民事手続き上での開示が可能である。

2.7.5　利用者の要求による情報開示

本 TSA は、利用者により本 TSA にすでに開示された情報への開示を当該利用者から求められた場合、その要求者がその情報を開示した本人かどうかを確認する手続きを経た上で、要求者への当該情報の開示を行う。

2.7.6　その他の理由に基づく情報開示

規定しない。

2.8 知的財産権

本規程は、アマノビジネスソリューションズの知的財産の一部を構成するものであり、商標法、著作権法、その他知的財産に関する法律で保護されており、一切のライセンス、譲渡、

その他の使用許可を認めない。所有者の書面による明示の許可が無ければ、アマノビジネスソリューションズの知的財産の使用は明示的に禁止する。また以下の各号に定めるものに関する権利は本 TSA に帰属し、利用者を含むその他の者には移転しない。

（1）タイムスタンプトークンの取得、検証を行うためのソフトウェア

（2）商標、標章、標識及びその他のマーク

2.9 個人情報の扱い

本 TSA は、本サービスの加入申請時に利用者が提供した個人情報に対し、本サービスを提供する為に必要な範囲内でのみこれを使用する。また不正な手段による個人情報の取得は行わない。また業務上必要な期間を経過した後は、個人情報の廃棄、又はその他の処理を行う。本 TSA は、個人情報への不正アクセス、個人情報の紛失、改ざん、漏洩、その他の危険に対し合理的な安全保護措置を講じる。個人情報の取扱いを第三者に委託する場合は、当該委託先が当該個人情報を安全に管理するよう、必要かつ適切な監督を行う。

3. 本人確認と認証

本 TSA は、「2.7.5 利用者の要求による情報開示」の規程に基づき本人確認手続きを行う必要のある場合を除き、本人確認又は認証は行わない。

4. 運用要件

4.1 タイムスタンプトークンの発行

本 TSA は、利用者の要求に応じて本 TSA にて時刻情報を付与し、改ざんを検知する為の電子署名データを発行する。本 TSA が運営するタイムスタンプユニットは、不慮の事故による停止及び本規程の「4.8.2 タイムスタンプユニットの時刻精度」に定めた時刻精度以下にならないように最大限の努力をする。

4.2 タイムスタンプの検証

タイムスタンプを検証する為には、タイムスタンプの対象となったデータのハッシュ値との照合及び、タイムスタンプトークンに施された電子署名の検証が必要となるが、それらは利用者の環境にて行われるものであり、本 TSA にて実施するものではない。

4.3 監査

4.3.1 監査情報の定義

監査情報とは、本規程、利用規約、システムイベント、当該 TA から発行された時刻監査の記録等の監査を行う為に必要な情報を言う。

4.3.2　監査人の身元、資格

監査人は、アマノビジネスソリューションズもしくはアマノ株式会社の従業員であり、本規程の「4.3.1　監査情報の定義」に定めた監査情報を取り扱う業務に精通した者から選出し、本 TSA の責任者が任命する。本 TSA は、必要に応じて外部の監査人を任命する。

4.3.3　監査人と被監査部門との関係

監査人は、本 TSA の運用部門に属さない者とする。

4.3.4　監査周期

監査の頻度は、最低年１度行う。

4.3.5　監査情報の保管期間

監査情報は、１０年以上保管する。

4.3.6　監査指摘事項への対応

監査指摘事項に対しては、本 TSA の責任者が判断し、場合により本サービスの運用を停止する事もある。本 TSA の責任者は指摘事項の改善作業の確認を行う。

4.3.7　監査情報の保護

本 TSA による監査情報及び監査結果の保存の為には、不正なアクセスによる情報の変更、改ざん、削除、漏洩等が無いよう適切かつ合理的な安全対策を講ずる。

4.3.8　監査情報の保管

監査情報は、そのアクセス権限を明確にし、不正アクセスによる情報の変更、改ざん、削除、漏洩等から保護され、必要に応じ適正な期間内に提供可能な状態で保管される。

4.3.9　監査結果の開示と対処

監査実施後、本 TSA は利用者の要求に応じて監査結果を速やかに開示するものとし、監査の結果として欠陥が指摘された場合には以下の対処を行う。

・欠陥が修正されるまでの対処（例えば運用の停止、利用者に対する十分なアナウンス等）
・欠陥への対処
・再発防止対策

4.4　記録のアーカイブ化

4.4.1　アーカイブデータの種類

本 TSA のアーカイブデータは次のものとする。

・当該 TA から発行された時刻監査証
・本 TSA で使用する鍵ペアの生成・更新破棄・失効記録
・監査報告書

4.4.2　アーカイブデータの保管期間
アーカイブデータは、１０年以上保管する。

4.4.3　**アーカイブデータの保護**
アーカイブデータにはアクセス制御を施すとともに、改ざん検出を可能とする措置を講ずる。
アーカイブデータのバックアップは、定期的に外部記憶媒体に取得し、適切な入退室管理が行われている室内に設置された施錠可能な場所に保管する。

4.4.4　アーカイブデータのバックアップ
アーカイブデータは、所定の方法、手順によりバックアップを行う。

4.4.5　記録へのタイムスタンプ要件
記録に時刻情報を付与するコンピュータのシステム時計は、UTC と同期させる。

4.4.6　アーカイブデータの収集システム
規定しない。

4.5　鍵の定期更新
タイムスタンプトークンの生成に関わる鍵ペアは、１年に１度定期的に更新を行う。

4.6　システムのトラブル、災害からの復旧
（１）本 TSA が使用するタイムスタンプシステムの時刻精度が、本規程の「4.8.2　タイムスタンプユニットの時刻精度」に規定する範囲外になった場合はシステムトラブルとみなし、タイムスタンプユニットを緊急停止し速やかに復旧作業を行う。本 TSA は、ハードウェア、ソフトウェア又はデータが破壊された場合、速やかに復旧作業を行う。
（２）本 TSA は、災害等により本 TSA の設備が被害を受けた場合、速やかに復旧作業を行う。
（３）システムのトラブルや災害などにより、サービスに支障を来たす事態が生じた場合には、速やかに認証局に通知し、その内容をホームページ上に公知する。

4.7　業務の終了
本 TSA がサービスを中断、終了する際は、そのスケジュールと手続きを決め、その内容を

ホームページ上に公知する。また、障害発生時などの予期出来ない場合の緊急停止措置以外は、事前の通知なしには業務を中断しない。

4.8　タイムソースの管理・トレーサビリティ

4.8.1　TSA 内の時刻精度

本 TSA は、本 TSA 内で稼動する全システムの時刻の精度を、当該 TA に対して 1 秒以内に維持する。

4.8.2　タイムスタンプユニットの時刻精度

本 TSA は、本 TSA が使用するタイムスタンプユニットの時刻精度を、当該 TA に対して 1 秒以内に維持する。

4.8.3　時刻のトレーサビリティ

本 TSA は、本 TSA が運営・管理するタイムスタンプユニットに対する時刻監査記録を当該 TA から取得・保管する事により、タイムスタンプトークンの時刻の UTC に対するトレーサビリティを保持する。

5.　物理的、手続き的及び要員的なセキュリティ管理

5.1　物理的なセキュリティ管理

5.1.1　施設の場所と建物構造

本サービスを運用するにあたって必要な設備は、地震、火災などの災害対策設計された施設内の施錠された区画内に設置する。

5.1.2　入退室管理と機器へのアクセス

本規程の「5.1.1　施設の場所と建物構造」で規定された施設に入館する者は、事前に登録が必要である。さらに施設の監視員と対面確認が必要であり機械による身体的特徴検査を受け、本人である事が確認出来た者のみ許可され入館出来る。退室時も同様の確認を行う。事前に登録の無い者は予め本 TSA の責任者より承認を受け、所定の手続きを行った後事前に登録され入館を許可された者と同伴で入館する。

5.1.3　電源、空調設備

本規程の「5.1.1　施設の場所と建物構造」で規定された施設の電源の瞬断には、ＵＰＳ設備が機能する。空調設備は常時運転され、設備機器に最適な温度に保たれる。

5.1.4　水害対策

規定しない。

5.1.5　火災対策

本規程の「5.1.1　施設の場所と建物構造」で規定された施設は、火災報知器により火災対策が施されている。

5.1.6　地震対策

本規程の「5.1.1　施設の場所と建物構造」で規定された施設は、免震又は耐震対策が施されている。

5.1.7　媒体管理

システムやデータをバックアップした記憶媒体は、空調とセキュリティが管理された場所に厳重に保管され、所定の手続きに基づき搬入出管理される。

5.1.8　廃棄物処理

機密扱いとみなす情報を含む書類、記憶媒体の廃棄については、厳密な分類の後適切に処理される。特に情報の格納に使用した全ての媒体は、破壊してから破棄処分する。

5.1.9　外部バックアップ

規定しない。

5.2　手続きの管理

5.2.1　信頼される役割

本 TSA の責任者より承認された各オペレータのシステムアクセスは、その業務遂行上実行しなければならない行為に限定される。本 TSA の責任者は、オペレータを兼務する事はできない。

5.2.2　人員配置

本 TSA の責任者は、業務に支障が出ない範囲内で人員配置を必要最小限にする。

5.2.3　各役割の認証と認可

全てのオペレータは、所定の手続きにより同一性を証明しシステムへのアクセスを許可される。

5.3　要員的なセキュリティ管理

5.3.1　従事者の要件

業務に従事する者については、人事情報により適格性の確認を行った後任命される。

5.3.2　経歴検査

本 TSA は、業務に従事する者について任命する前に信頼性、適格性を確認する為の調査を行う。

5.3.3　トレーニング要件

本 TSA は、運用に必要な知識取得の為要員に対しトレーニングを行う。

5.3.4　トレーニング周期

本 TSA は、要員に対するトレーニングを計画に基づき実施する。

5.3.5　ジョブローテーションの実施

本 TSA は、要員のジョブローテーションを必要に応じて行う。

5.3.6　不正行為の罰則

要員が、規定された権限より逸脱して違反を行った場合は、就業規則、契約等に基づき　　処分を行う。

5.3.7　要員へ提示する文書

本 TSA は、それぞれの職務に必要な文書を提示する。
運用規定、機器類のマニュアル、手順書等。

6　技術的管理

6.1　鍵ペア生成とインストール

6.1.1　鍵ペア生成

本 TSA による鍵ペアの生成は、鍵管理モジュールにおいて複数人管理の下で行われる。

6.1.2　タイムスタンプトークンの公開鍵証明書の配布

タイムスタンプトークンに使用される公開鍵証明書は、リポジトリにて公開される。

6.1.3　鍵長

タイムスタンプトークンの秘密鍵には、RSA 2048 bit 以上の鍵を使用する。

6.1.4　鍵生成

タイムスタンプトークンに関わる鍵ペアの生成は、本規程の「6.2.1　暗号モジュールの基準」で定められたハードウェアで行う。

6.1.5　鍵使用の目的

本 TSA は、タイムスタンプトークンの発行に必要な署名の為に鍵を用いる。

6.2　秘密鍵の防護

6.2.1　暗号モジュールの基準

タイムスタンプユニット秘密鍵は、FIPS 140-2 Level 3 以上の HSM により保護される。

6.2.2　秘密鍵の複数人管理

タイムスタンプユニットの秘密鍵の生成、破棄を行う際は、複数の鍵管理者の下で行う。また、生成、破棄の方法と手順については、所定の手続きに従う。

6.2.3　秘密鍵の預託

本 TSA は、秘密鍵の預託を行わない。

6.2.4　秘密鍵のバックアップ

本 TSA は、タイムスタンプユニットの秘密鍵のバックアップを行わない。

6.2.5　秘密鍵のアーカイブ

本 TSA は、秘密鍵のアーカイブを行わない。

6.2.6　暗号モジュールへの秘密鍵格納

本 TSA の秘密鍵は、暗号モジュール内で生成され格納される。

6.2.7　秘密鍵活性化方法

本 TSA の秘密鍵は、定められた鍵管理者により暗号モジュールに PIN 入力して活性化される。

6.2.8　秘密鍵非活性化方法

本 TSA の秘密鍵は、定められた鍵管理者により暗号モジュールに PIN 入力して非活性化される。

6.2.9　秘密鍵破棄方法

暗号モジュール内の秘密鍵の破棄は、複数の鍵管理者の下、暗号モジュールの鍵更新操作によって行われる。尚、暗号モジュールを破棄目的等で室外に持ち出す場合には、複数の鍵管理者の下で所定の手続きに従い破棄を実施する。

6.3　その他の鍵管理について

6.3.1　公開鍵記録保存

本 TSA の公開鍵は、本規程の「4.4.2　アーカイブデータの保管期間」において定める期間、保管する。

6.3.2　秘密鍵の使用期間

本 TSA の秘密鍵の使用期間は 1 年とし、鍵ペアを生成し活性化した日から起算して 1 年毎に鍵更新を行う。また、鍵の危殆化が判明した場合には、その時点で公開鍵証明書の失効手続きを行う。

6.3.3　鍵ペアの有効期間

本 TSA の鍵ペアの有効期間は、11 年 1 ヶ月間とする。但し、秘密鍵の危殆化や、ハッシュ及び暗号アルゴリズムの脆弱化が発生した場合には、タイムスタンプトークンに示される有効期限より以前に、その有効性を失効させる事がある。

6.4　活性化データ

6.4.1　活性化データの生成

本 TSA は、秘密鍵を格納する暗号モジュールの操作に必要な活性化データを、所定の手続きにより生成する。

6.4.2　活性化データの保護

本 TSA は、秘密鍵を格納する暗号モジュールの活性化に必要な PIN などの情報を安全に管理する。

6.5　コンピュータセキュリティ管理

6.5.1　使用するコンピュータセキュリティの技術要件

本 TSA の装置やソフトウェアは、セキュリティ条件を満たすものを導入する。

6.5.2　コンピュータセキュリティ評価

本サービスを運用する為に必要な全ての機器類に対して、定期的にセキュリティの脆弱性評価を行い、問題がある場合は対処する。また、機器類に変更があった場合においても同様の手続きを行う。

6.6　システムのライフサイクル管理

6.6.1　システム開発管理

本 TSA は、使用されるソフトウェアの開発、修正、変更を品質管理された環境で行う。

6.6.2　システム維持管理

本 TSA は、使用される機器及びソフトウェアの維持管理を行い、保守体制を備える。

6.6.3　セキュリティ運用管理

本 TSA は、ハードウェアやソフトウェアの導入時に、セキュリティの確認調査を行う。

6.6.4　セキュリティ評価のライフサイクル

本 TSA は、定期的にセキュリティの脆弱性評価を行い、問題がある場合は対処する。

6.7　ネットワークセキュリティ管理

本 TSA は、システム導入時、運用時、変更時においてネットワークセキュリティが確保されているかどうかの確認を行う。

6.8　暗号化モジュールの管理

本 TSA は、暗号モジュールに FIPS 140-2 Level 3 認定品を使用する。

7.　仕様の管理

7.1　仕様の変更手順

本規程の仕様は、必要に応じて変更する。

7.2　公開と通知の規則

本規程の変更時は、速やかに新しい規程をリポジトリに公開する。

7.3　本規定の承認手順

本規程の変更は、本 TSA の責任者により承認される。

8. タイムスタンプトークンのプロファイル

フィールド	内容	値
TimeStampToken		
ContentInfo		
ContentType	content(データ)の型	id-signedData (OID:1.2.840.113549.1.7.2)
Content		
version	CMSのバージョン	3
digestAlgorithms	署名に使用するダイジェストアルゴリズムの識別子	sha1 (OID:1.3.14.3.2.26) sha256 (OID:2.16.840.1.101.3.4.2.1) sha384 (OID:2.16.840.1.101.3.4.2.2) sha512 (OID:2.16.840.1.101.3.4.2.3) ※注1
encapContentInfo		
eContentType	署名の対象となるデータの型	id-smime-ct -TSTInfo (OID:1.2.840.113549.1.9.16.1.4)
eContent	署名の対象となるデータ	TSTInfo(後述参照)
certificates	署名の検証に必要な証明書のリスト	※OPTIOANAL
certificate	TSAの公開鍵証明書	
attrCert	TAの時刻監査証明書	
signerInfos	署名者に関する情報	
version	CMS のバージョン	1
sid	署名者(TSA)を識別するための情報	
digestAlgorithm	署名に使用するダイジェストアルゴリズムの識別子	sha1,sha256,sha384,sha512 ※注1
signedAttrs	署名の属性	
Attribute		
attrType	属性のタイプ	ContentType (OID:1.2.840.113549.1.9.3)
AttributeValue	属性の値	id-smime-ct-TSTInfo (OID:1.2.840.113549.1.9.16.1.4)
Attribute		
attrType	属性のタイプ	messageDigest (OID:1.2.840.113549.1.9.4)
AttributeValue	属性の値	署名の対象となるデータのハッシュ値
Attribute		
attrType	属性のタイプ	id-aa-signingCertificate (OID:1.2.840.113549.1.9.16.2.12)
AttributeValue	属性の値	
SigningCertificate	証明書署名	
signatureAlgorithm	署名に使用するアルゴリズム	sha1WithRSAEncryption (OID:1.2.840.113549.1.1.5) sha256WithRSAEncryption (OID:1.2.840.113549.1.1.11) sha384WithRSAEncryption (OID:1.2.840.113549.1.1.12) sha512WithRSAEncryption (OID:1.2.840.113549.1.1.13) ※注1
signature	署名値	
TSTInfo		
version	タイムスタンプトークンフォーマットバージョン	1
TSAPolicyId	サービスポリシーの識別子	(OID:0.2.440.200217.100.200.100)
messageImprint		
hashAlgorithm	ハッシュアルゴリズム	sha1,sha256,sha384,sha512
hashedMessage	タイムスタンプ対象のハッシュ値	
serialNumber	タイムスタンプトークンのシリアル番号	
genTime	タイムスタンプトークン生成時の時刻情報	YYYYMMDDhhmmss[sss]Z
accuracy	時刻精度	msec
ordaring	タイムスタンプトークン発行の順序性の有無	FALSE
nonce	特定の要求を識別するための値	ランダム値
tsa	タイムスタンプユニットの識別情報	C=JP; S=Kanagawa; L=Yokohama; O=AMANO Time Business Corporation; OU=e-timing Free TSA; OU=nCipher DSE ESN:????-????-????; CN=dse200-F???
extensions	拡張領域	使用しない
※注1　TSTInfo中のハッシュアルゴリズムと同一のものが適用されます。		

用語集 A

用語	スペル	解説
FIPS 140-2	Federal Information Processing Standard 140-2	米国 NIST が策定した暗号モジュールに関するセキュリティ認定基準。最低レベル 1 から最高レベル 4 まである。
HSM	Hardware Security Module	ハードウエアセキュリティモジュール。物理的に暗号モジュール等の機密性を保護する装置。分解したり、衝撃を加えたりすると装置内のデータが消失する仕掛けになっているものや、温度変化や気圧の変化を検出するものもある。
IETF	Internet Engineering Task Force	インターネットで使用されるプロトコルを決定する為の民間主導の標準化団体。IETF から RFC 番号がつけられて公表された規格は、実質的に世界標準規格である。
PIN	Personal Identification Number	個人認識番号。
UPS	Uninterruptible power supply	様々な電源トラブルを取り除き、サーバ・ネットワーク機器等のシステム全体にクリーンかつ 高品質の電源供給を行い、貴重なデータの消失を防止する為の装置。
UTC	Coordinated Universal Time	協定世界時。現在全世界で公式に採用されている原子時系。UTC は実時間では生成出来ず、各国の国家時刻標準機関が生成する協定世界時を基に国際相互比較し、後日それらのデータを集計し計算により決定される。
公開鍵暗号基盤	Public Key Infrastructure	公開鍵暗号技術と電子署名を使って、インターネットで安全な通信が出来るようにする為の環境の事。
時刻監査		対象となる装置の時刻を監視し、標準時とのズレを検査する事。
時刻同期		基準となる時刻に対象装置の時刻を合わせる事。
身体的特徴		本人認証では、虹彩、手のひらの血流、指紋、声紋などが用いられる。

用語集 B

用語	スペル	解説
タイムスタンプ	Time Stamp	信頼の置ける時刻と文書などのデジタル情報に対し、変更、改ざんがあったかどうかを検知出来る情報もしくはそれを指し示す情報を付与し、それ以降、内容や時刻に変更・改ざんがあったかどうかを証明する技術。
TSA	Time-Stamping Authority	タイムスタンプサービスを提供し、第三

		者機関としてタイムスタンプ記録を発行、検証するサービスプロバイダ。
タイムスタンプトークン	Time-Stamp Token	信頼の置ける時刻と文書などのデジタル情報に対し、変更、改ざんがあったかどうかを検知出来る情報。もしくはそれを指し示す情報。デジタル情報のハッシュデータに時刻情報等を付与し、電子署名として発行する。タイムスタンプトークンには独立トークンとリンクトークンの二種類が存在し、それぞれISO/IEC18014-2,3 に規定されている。
タイムソース	Time Source	時刻源の事を言う。
トレーサビリティ	Traceability	トレーサビリティとは、「不確かさが全て表記された、切れ目の無い比較の連鎖を通じて、通常は国家標準又は国際標準である決められた標準に関連づけられ得る測定結果又は 標準の性質」を言う。 VIM（国際計量基本用語集）より抜粋
リポジトリ	Repository	ここでは本規程などの情報を保存・配布出来るようにしたオンライン上のデータベースの事。